THREATS TO USERS OF ADULT WEBSITES IN 2018

February 2019

CONTENTS

INTRODUCTION

2018 was a year that saw campaigns to decrease online pornographic content and traffic. For example, one of the most adult-content friendly platforms – Tumblr – announced it was banning erotic content (even though almost a quarter of its users consume adult content). In addition, the UK received the title of 'The Second Most Porn-Hungry Country in the World' and is now implementing a law on age-verification for pornography lovers that will prohibit anyone below the age of 18 to watch this sort of content. This is potentially opening a world of new tricks for scammers and threat actors to take advantage of users. In addition, even commercial giant Starbucks declared a 'holy war' on porn as it was revealed that many visitors prefer to have their coffee while consuming adult content, rather than listening to music or reading the latest headlines on news websites.

Such measures might well be valid, at least from a cybersecurity perspective, as the following example suggests. According to news reports last year, an extremely active adult website user, who turned out to be a government employee, dramatically failed to keep his hobby outside of the workplace. By accessing more than 9,000 web pages with adult content, he compromised his device and subsequently infected the entire network with malware, leaving it vulnerable to spyware attacks. This, and other examples confirm that adult content remains a controversial topic from both a social and cybersecurity standpoint.

It is no secret that digital pornography has long been associated with malware and cyberthreats. While some of these stories are now shown to be myths, others are very legitimate. A year ago, we conducted research on the malware hidden in pornography and found out that such threats are both real and effective. One of the key takeaways of last year's report was the fact that cybercriminals not only use adult content in multiple ways – from lucrative decoys to make victims install malicious applications on their devices, to topical fraud schemes used to steal victims' banking credentials and other personal information – but they also make money by stealing access to pornographic websites and reselling it at a cheaper price than the cost of a direct subscription.

Last year, we discovered a number of malicious samples that were specifically hunting for credentials to access some of the most popular pornographic websites. When we considered why someone would hunt for credentials to pornographic websites, we checked the underground markets (both on the dark web and on open parts of the internet) and found that credentials to pornography website accounts are themselves quite a valuable commodity to be sold online. They are for sale in their thousands.

It would be going too far to say that the findings from our previous exploration of the relationships between cyberthreats and adult content were unexpected. At the end of the day, pornography has always been, and remains one of the most sought after types of online content. At the same time, cybercriminals have always looked to increase their profits with the most efficient and cheapest way of delivering malicious payloads to victims. It was almost inevitable that adult content would become an important tool for them.

That said, our monitoring of the wider cyberthreat landscape shows that threat actors tend to change their habits, tactics and techniques over time. This means that even in a niche area, such as pornographic content and websites, changes are possible. That is why this year we decided to repeat our exercise and investigate the topic once again. As it turned out, some things have indeed changed.

METHODOLOGY AND KEY FINDINGS

To measure the level of risk that may be associated with adult content online, we investigated several different indicators. We examined malware disguised as pornographic content, and malware that hunts for credentials to access pornography websites. We looked at the threats that are attacking users across the internet in order to find out which popular websites might be dangerous to visit. Additionally, we checked our phishing and spam database to see if there is a lot of pornographic content on file and how is it used in the wild. Using aggregated threat-statistics obtained from the Kaspersky Security Network – the infrastructure dedicated to processing cybersecurity-related data streams from millions of voluntary participants around the world – we measured how often and how many users of our products have encountered adult-content themed threats.

Additionally, we checked around twenty underground online markets and counted how many accounts are up for sale, which are the most popular, and the price they are sold for.

As a result, we discovered the following:

- **Searching for pornography online has become safer**: in 2018, **650,000 users** faced attacks launched from online resources. That is **36% less** than in 2017 when more than a million of these attacks were detected.
- **Cybercriminals are actively using popular porn-tags to promote malware in search results**. The 20 most popular make up 80% of all malware disguised as porn. Overall, 87,227 unique users downloaded porn-disguised malware in 2018, with 8% of them using a corporate rather than personal network to do this.
- **In 2018, the number of attacks using malware to hunt for credentials that grant access to pornography websites grew almost three-fold compared to 2017**, with more than 850,000 attempts to install such malware. The number of users attacked doubled, with 110,000 attacked PCs across the world.
- The number of **unique sales offers of credentials for premium accounts to adult content websites almost doubled** to more than **10,000**.
- **Porn-themed threats increased in terms of the number of samples, but declined in terms of variety**: In 2018, Kaspersky Lab identified at least **642 families of PC threats** disguised under one common pornography tag. In terms of their malicious function, these families were distributed between **57 types** (76 last year). In most cases they are are **Trojan-Downloaders, Trojans and AdWare**.
- **89%** of infected files disguised as pornography on Android devices turned out to be **AdWare**.

- In Q4 2018, there were 10 times as many attacks coming from phishing websites pretending to be popular adult content resources, compared to Q4 2017 when the overall figure reached **21,902 attacks**.

PART 1 – MALWARE

As mentioned above, cybercriminals put a lot of effort into delivering malware to user devices, and pornography serves as a great vehicle for this. Most malware that reaches users' computers from malicious websites is usually disguised as videos. Users who do not check the file extension and go on to download and open it, are sent to a webpage that extorts money. This is achieved by playing the video online or for free only after the user agrees to install a malicious file disguised as a software update or something similar. However, in order to download anything from this kind of website, the user first has to find the website. That is why the most common first-stage infection scenarios for both PC and mobile porn-disguised malware involve the manipulation of search query results.

To do this, cybercriminals first identify which search requests are the most popular among users looking for pornography. They then implement so-called 'black SEO' techniques. This involves changing the malicious website content and description so it appears higher up on the search results pages. Such websites can be found in third or fourth place in the list of search results.

According to our findings, this method is still actively used but its efficiency is falling. To check this, we took 100 of the top listed pornographic websites (as suggested by search engines after entering a query for the word 'porn'), plus those that have the word 'porn' in the title. We checked if any of them pose any threat to users. It turned out that in 2017 our products stopped more than a million users from attempting to install malware from websites on the list. However, in 2018, the number of users affected decreased to 658,930. This could be the result of search engines putting processes in place to fight against 'black SEO' activities and protecting users from malicious content.

Porn tags = Malware tags

Optimizing malicious websites so as to ensure that those wanting to view adult content will find them is not the only tool criminals explore in order to find the best ways of delivering infected files to victims' devices. It turned out during our research that cybercriminals are disguising malware or not-a-virus files as video files and naming them using popular porn tags. A 'porn tag' is a special term that is used to easily identify content from a specific pornographic video genre.

Tags are used by pornography websites to organize their video libraries and help users to quickly and conveniently find the video they are interested in. The not-a-virus type of threats is represented here by RiskTools, Downloaders and AdWare. Each type is not typically classified as malware, yet such applications

may do something unwanted to users. AdWare, for instance, can show users unsolicited advertising, alter search results and collect user data to show targeted, contextual advertising.

To check how widespread this trend is, we took the most popular classifications and tags of adult videos from three major legal websites distributing adult content. The groupings were chosen by the overall number of videos uploaded in each category on the websites. As a result, we came up with a list of around 100 tags, which between them may well cover every possible type of pornography in existence. Subsequently, we ran those tags against our database of threats and through the Kaspersky Security Network databases and figured out which of them were used in malicious attacks and how often.

The overall number of users attacked with malware and not-a-virus threats disguised as porn-themed files dropped by about half compared to 2017. While back then their total number was 168,702, the situation in 2018 was a little more positive: down to 87,227, with 8% of them downloading porn-disguised malware from corporate networks. In this sense, scammers are merely following the overall trend: according to Pornhub's statistics, the share of pornography viewed on desktops has dropped by 18%. However, we were not able to get full confirmation that the 2018 decrease in the number of users attacked with malicious pornography relates to changes in consumer habits.

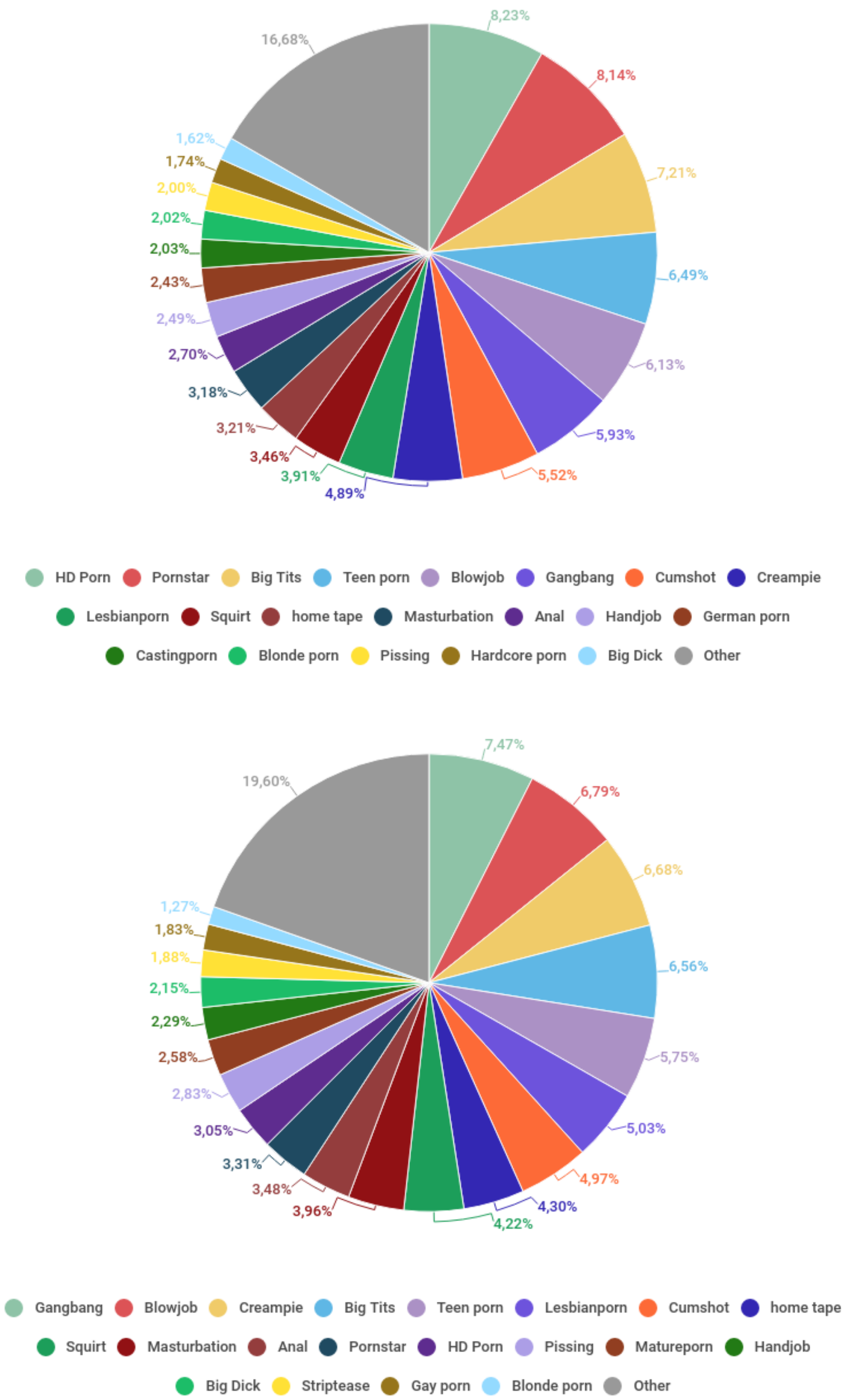


Fig.1: Top-20 porn-related categories that were used as a disguise for porn-related files by the number of attacked users in 2017 and 2018 on a pie-chart.
Source: Kaspersky Security Network

Perhaps one of the most interesting takeaways we got from the analysis of how malware and not-a-virus are distributed among porn tags, is that although we were able to identify as many as 100 of them, most of the attacked users (around 80%, both in 2017 and 2018) encountered threats that mention only 20 of them. The tags used most often match the most popular tags on legitimate websites. Although we couldn't find perfect correlations between the top watched types of adult video on legitimate websites and the most often encountered porn-themed threats, the match between malicious pornography and safe pornography means that malware and not-a-virus authors follow trends set by the pornography-viewing community.

Moving forward, the overall picture surrounding porn-disguised threat types showed more changes in 2018 when compared to 2017. In 2018, we saw 57 variations of threats disguised as famous porn tags, from 642 families. For comparison, the figures in 2017 were 76 and 581 respectively. That means that while the number of samples of porn-malware is growing, the number of types of malware and not-a-virus that are being distributed through pornography is decreasing.

The top three most popular classes of threats turned out to be Trojan-Downloader, with 45% of files, Trojan with 20% and AdWare, which is not a virus, with 9%, while in 2017 the top three were different: Trojan-Downloader was still there with 29%, exploits took the second place with 23% and Trojans accounted for around 19%.

Distribution of porn-themed threat types in 2017

Distribution of porn-themed threat types in 2018

Trojan-Downloader	**29%**	Trojan-Downloader	**45%**
Exploit	**23%**	Trojan	**20%**
Trojan	**19%**	AdWare (not a virus)	**9%**
AdWare (not a virus)	**11%**	Worm	**8%**
Worm	**6%**	Virus	**2%**
Virus	**2%**	Downloader (not a virus)	**2%**
RiskTool (not a virus)	**2%**	Exploit	**2%**
Downloader (not a virus)	**2%**	Trojan-Dropper	**2%**
Trojan-Dropper	**1%**	UDS: DangerousObject	**2%**
Other	**5%**	Other	**8%**

Fig.2: Top-10 types of threat that went under the disguise of porn-related categories, by the number of attacked users in 2017 and 2018. Source: Kaspersky Security Network

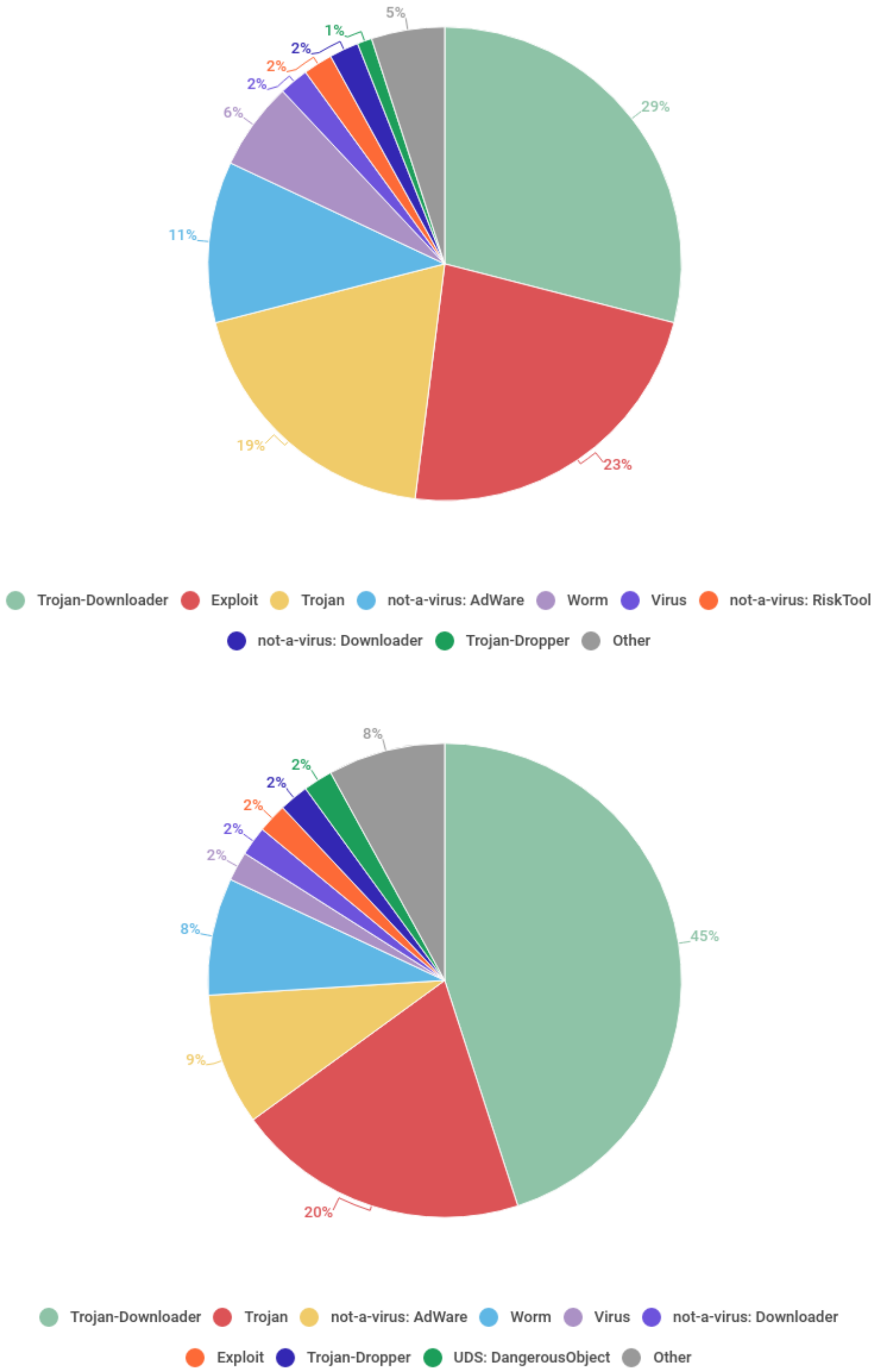


Fig.3: Top-10 verdicts which went under the disguise of porn-related categories, by the number of attacked users in 2017 and 2018. Source: Kaspersky Security Network

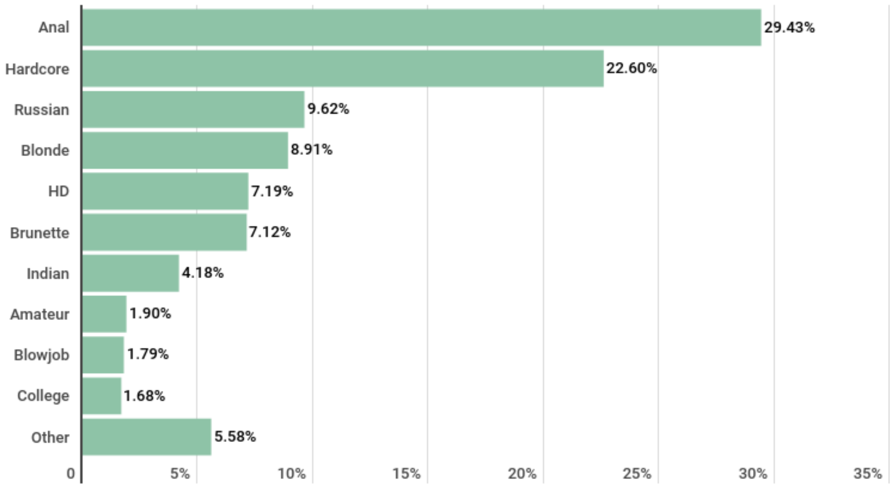
The most noticeable change in the overall picture is the large number of exploits in 2017: back then they accounted for almost a quarter of all infected files, while in 2018 they were not represented in the top 10. There is an explanation for the popularity of such threats. In 2017, exploits were represented by massive detections of Exploit.Win32.CVE-2010-2568.gen, a generic detection (the detection that describes multiple similar malware pieces) for files that exploited the vulnerability in the Windows Shell named CVE-2010-2568. However, the same detection name applies for another vulnerability in LNK – CVE-2017-8464. This vulnerability, and the publicly available exploit for it, became public in 2017 and immediately raised a lot of interest amongst threat actors – thereby raising the bar in exploit detections. Within a year, the attacks on CVE-2017-8464 reduced significantly as most users patched their computers and malware writers went back to using classical malware aimed at more common file formats (such as JS, VBS, PE).

The rise in popularity of Trojan-Downloaders can be explained by the fact that such malicious programs are multipurpose: once installed on a victim's device, the threat actor could additionally download virtually any payload they want: from DDoS-bots and malicious ads clickers to password stealers or banking Trojans. As a result, a criminal would need to infect the victim's device only once and would then be able to use it in multiple malicious ways.

2018 has also seen some changes in the share of software that is not-a-virus. All in all, such programs accounted for 15% of all threats in 2017. In 2018, however, they were on the decline and now account for 11%, with downloaders losing their place in the top-10 most prolific threats. So, while the attackers are using porn less as a decoy, they have yet to inject the malicious files with more harmful threats, such as Trojans and worms.

Mobile malware

Following technical changes in how we detect and analyze mobile malware, we amended our methodology for this report. Instead of trying to identify the share of porn-themed content in the overall volume of malicious applications that our users encountered, we selected 100,000 random malicious installation packages disguised as porn videos for Android, in 2017 and 2018, and checked them against the database of popular porn tags.



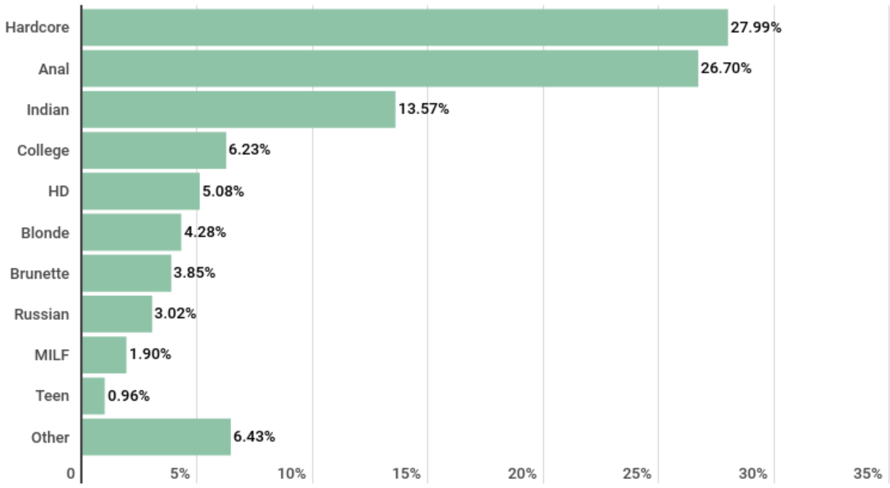


Fig.4: Top-10 porn-related categories that were used as a disguise for porn-related files by the number of attacked mobile users in 2017. Source: Kaspersky Security Network

The landscape for types and families of mobile threats is also different than for PC. In both 2017 and 2018, the most common type of threat was AdWare: 70% in 2017 and 89% in 2018.

Malware name	%	Malware name	%
not-a-virus:HEUR:AdWare.AndroidOS.Agent.n	**59.61%**	not-a-virus:HEUR:AdWare.AndroidOS.Agent.f	**62.88%**
not-a-virus:HEUR:AdWare.AndroidOS.Ewind.h	**11.02%**	not-a-virus:HEUR:AdWare.AndroidOS.Agent.n	**17.09%**
HEUR:Trojan-Ransom.AndroidOS.Zebt.a	**5.33%**	not-a-virus:HEUR:AdWare.AndroidOS.Ewind.h	**9.62%**
HEUR:Trojan.AndroidOS.Loapi.b	**3.76%**	HEUR:Trojan-Ransom.AndroidOS.Zebt.a	**3.27%**
HEUR:Trojan-Ransom.AndroidOS.Small.snt	**2.22%**	HEUR:Trojan.AndroidOS.Boogr.gsh	**0.74%**
HEUR:Trojan-Dropper.AndroidOS.Agent.hb	**1.93%**	HEUR:Trojan-Ransom.AndroidOS.Small.snt	**0.74%**
not-a-virus:HEUR:AdWare.AndroidOS.Agent.f	**1.90%**	UDS:DangerousObject.Multi.Generic	**0.52%**
HEUR:Trojan-Ransom.AndroidOS.Small.as	**1.54%**	HEUR:Trojan-Ransom.AndroidOS.Small.as	**0.41%**
HEUR:Trojan-Ransom.AndroidOS.Small.cj	**1.29%**	not-a-virus:HEUR:AdWare.AndroidOS.Ewind.cx	**0.36%**
not-a-virus:HEUR:AdWare.AndroidOS.Ewind.cx	**1.07%**	HEUR:Trojan-Ransom.AndroidOS.Small.cj	**0.36%**

Fig.5: Top-10 verdicts that represent porn-related categories, by the number of attacked mobile users, in 2017 and 2018. Source: Kaspersky Security Network

These threats are typically distributed through affiliate programs focused on earning money as a result of users installing applications and clicking on an advertisement. As well as AdWare, pornography is also used to distribute ransomware (4% in 2018) but on a much smaller scale compared to 2017, when more than 10% of users faced such malicious programs. This decline is most likely a reflection of the overall downward trend for ransomware seen in the malware landscape.

Credential hunters

A specific type of malware related to pornography, which we have been tracking throughout the year, is implemented by so-called credential hunters. We track them with the help of our botnet-tracking technology, which monitors active botnets and receives intelligence on what kind of activities are they perform, to prevent emerging threats.

We particularly track botnets that are made of malware.Upon installation on a PC, this malware can monitor which web pages are opened, or create a fake one where the user enters their login and password credentials. Usually such programs are made for stealing money from online banking accounts, but last year we were surprized to discover that there are bots in these botnets that hunt for credentials to pornography websites.

Based on the data we were able to collect, in 2017 there were 27 variations of bots, belonging to three families of banking Trojans, attempting to steal credentials (Betabot, Neverquest and Panda). These Trojans were after credentials to accounts for 10 famous adult content websites (Brazzers, Chaturbate, Pornhub, Myfreecams, Youporn, Wilshing, Motherless, XNXX, X-videos). During 2017, these bots attempted to infect more than 50,000 users over 307,000 times.

In 2018, the number of attacked users doubled, reaching more than 110,000 PCs across the world. The number of attacks almost tripled, to 850,000 infection attempts. At the same time, the number of variations of malware we were able to spot fell from 27 to 22, but the number of families increased from three to five, meaning that pornography credentials are considered valuable to ever more cybercriminals.

Another important shift that happened in 2018, was that malware families do not hunt for credentials to multiple websites. Instead, they focus on just two: mostly Pornhub and XNXX, whose users were targeted by bots belonging to the Jimmy malware family.

Apparently Pornhub remains popular, not only to regular users of the web, but also to cybercriminals looking for another way of gaining illegal profits by selling user credentials.

PART 2 – PHISHING AND SPAM

Our previous research suggested that it is relatively rare to see pornography as a topic of interest in phishing scams. Instead, criminals prefer to exploit popular sites dedicated to finding sex partners. But in 2018, our anti-phishing technologies started blocking phishing pages that resemble popular pornography websites.

These are generally pages disguised as pornhub.com, youporn.com, xhamster.com, and xvideos.com. In Q4, 2017, the overall number of attempts to access phishing pages pretending to be one of the listed websites was **1,608**. Within a year, in Q4 2018, the number of such attempts (**21,902**) was more than ten times higher.

The overall number of attempts to visit phishing webpages pretending to be one of the popular adult-content resources was **38,305**. Leading the list of accessed phishing pages were those that were disguised as a Pornhub page. There were **37,144** attempts to visit the phishing version of the website, while there were only **1,161** attempts to visit youporn.com, xhamster.com, and xvideos.com in total. These figures are still relatively low, other phishing categories may see detection results of millions of attempts per year. However, the fact that the number of detections on pornography pages is growing may mean that criminals are only just beginning to explore the topic.

It is worth mentioning that phishing pages cannot influence the original page in any way; they merely copy it. The authentic Pornhub page is not connected to the phishing. Moreover, most search engines usually successfully block such phishing pages, so the most likely way to access them is through phishing or spam e-mails, or by being redirected there by malware or a malicious frame on another website.

Fake versions of popular pornography websites target users' credentials and contact details, which can later be either sold or used in other fraud schemes or cyberattacks. In general, credentials capture is one of the most popular ways to target users, using pornography to

> Although the number of phishing may seem high, it's important to note that in relation to the amount of site visits (33.5 billion visits in 2018), the percentage of phishing attempts is very small (less than .0001%). This low percentage rate can be attributed to the fact that Pornhub actively monitors and removes phishing websites and offers two-factor authentication when logging into PornHub accounts.
>
> To protect yourself from a phishing attack:
>
> - Do not click on malicious phishing links in your e-mails: we never send unsolicited emails or text messages asking for confidential information, such as a password;
> - When in doubt, go to Pornhub.com instead of clicking a link, such as in an email;
> - Always check that the domain name is Pornhub.com;
> - Always check that your connection is using HTTPS and that the certificate is valid
> - Report any suspicious activity to security@pornhub.com.

implement phising fraud schemes. In such schemes, the victim is often lured to a phishing website disguised as a social network, where they are asked to authenticate their identity in order to watch an adult video which can only be accessed if the user confirms they are over 18-years-old.

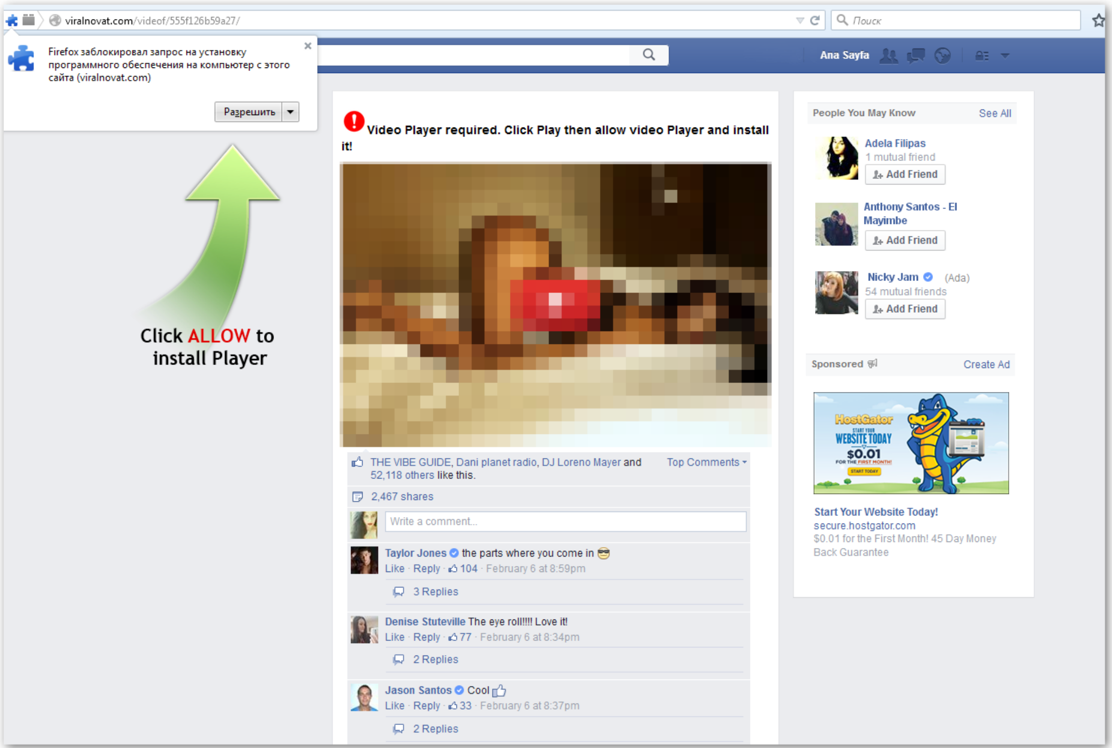


Fig.6: Screenshot of a porn-related phishing website (edited due to sensitive content). Source: Kaspersky Security Network

As the victim enters their password, the threat actor captures the credentials to the user's social network account.
Pornographic content phishing can also be used to install malicious software. For example, to access an alleged adult video, the phishing page requires the user to download and update a video player.

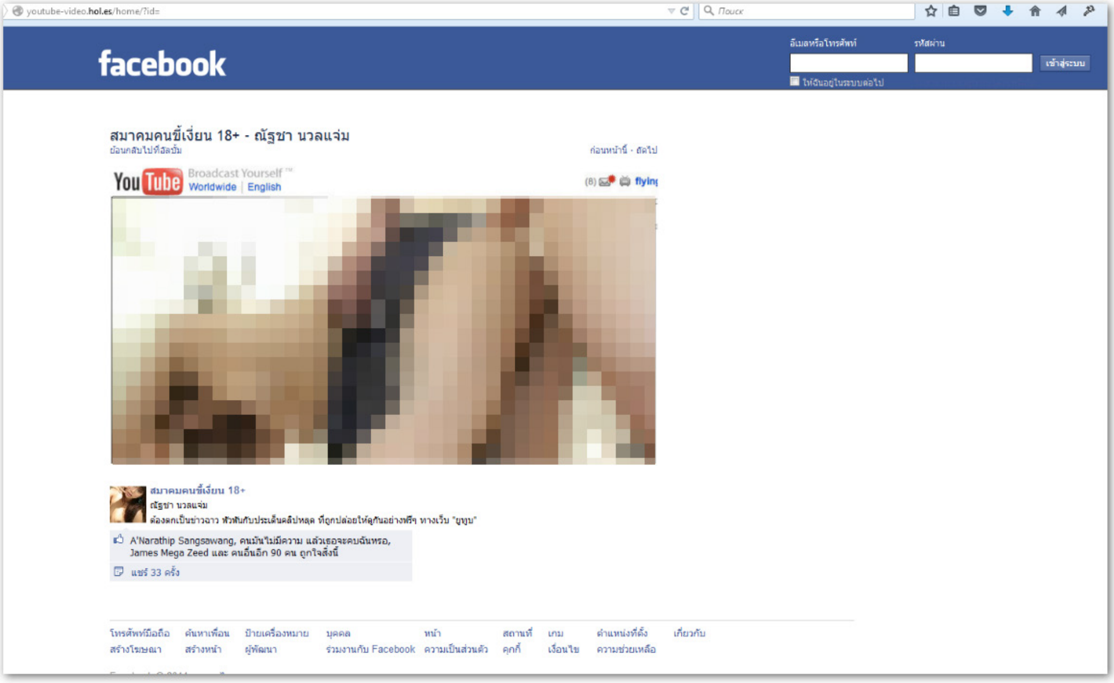


Fig.7: Screenshot of a porn-related phishing website (edited due to sensitive content). Source: Kaspersky Security Network

Needless to say, instead of downloading a video player, the user downloads malware.

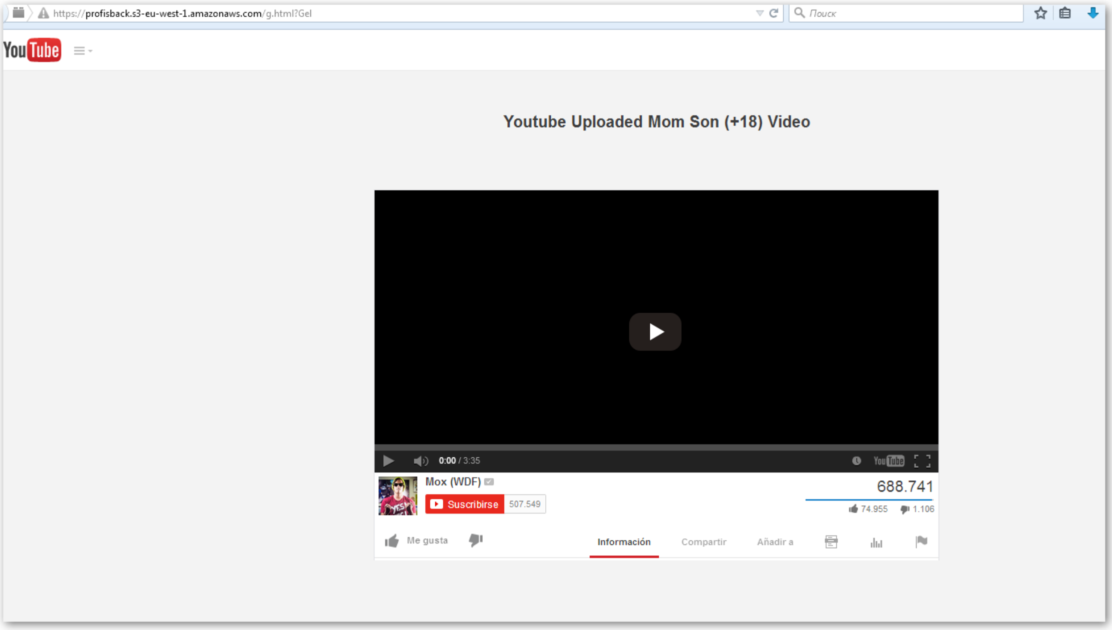


Fig.8: Screenshot of a porn-related phishing website (edited due to sensitive content).
Source: Kaspersky Security Network

Sometimes phishing fraudsters target e-wallet credentials with the help of pornographic content. The victim is lured to the pornographic website to watch a video broadcast. In order to view the content, the user is asked to enter their payment credentials.

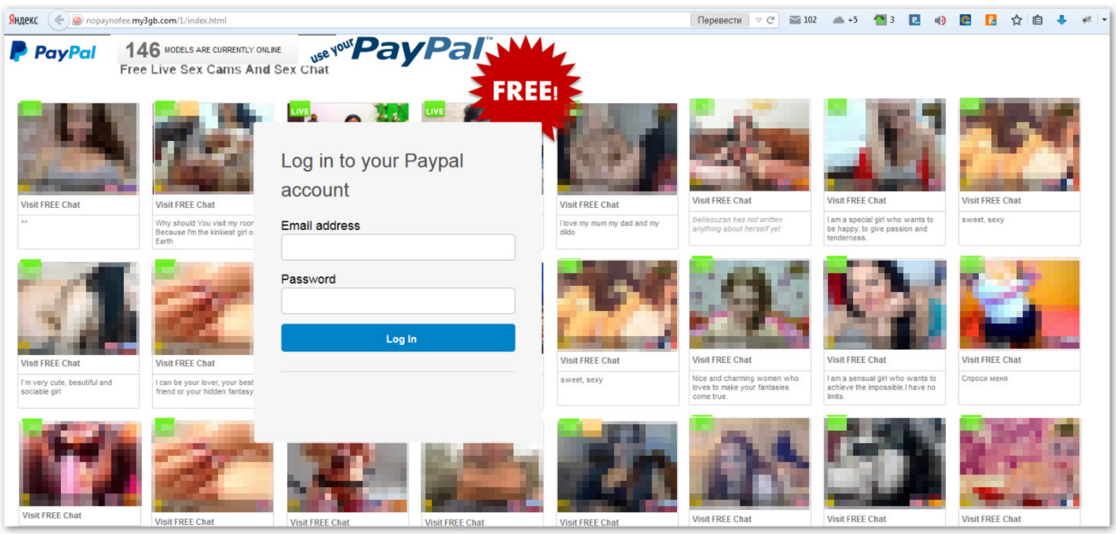
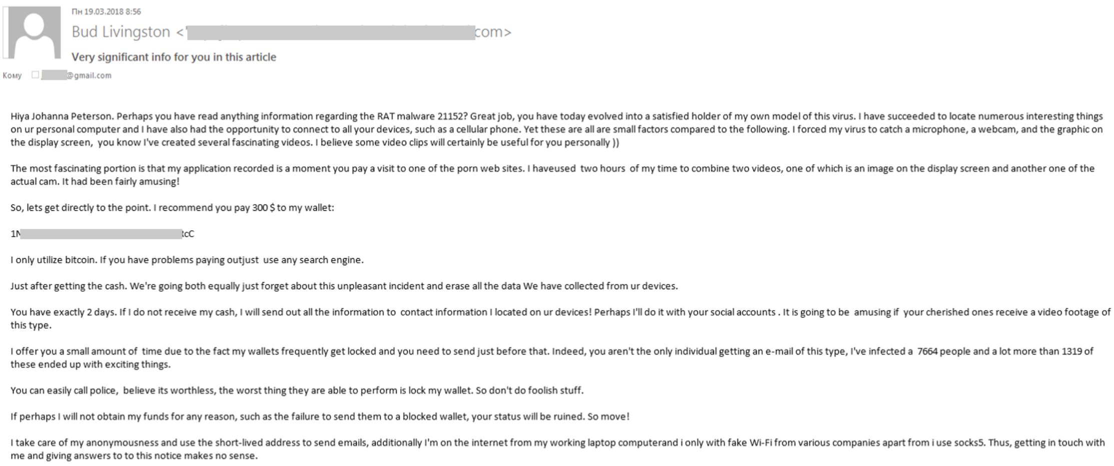


Fig.9: Screenshot of a porn-related phishing website (edited due to sensitive content).
Source: Kaspersky Security Network

Spam-scam

We have rarely seen pornographic content used in any special or specific way when it comes to spam. Apart from the mass distribution of 'standard' advertising offering adult content on legitimate and illegal websites, this type of threat hasn't been spotted using pornography in a creative way. However, there is one exception. Beginning in 2017, an infamous sextortion scam started to happen. Users started to receive messages containing an extortion letter with a demand to transfer bitcoins to fraudsters.



Пн 19.03.2018 8:56
Bud Livingston <[redacted]com>
Very significant info for you in this article
Кому [redacted]@gmail.com

Hiya Johanna Peterson. Perhaps you have read anything information regarding the RAT malware 21152? Great job, you have today evolved into a satisfied holder of my own model of this virus. I have succeeded to locate numerous interesting things on ur personal computer and I have also had the opportunity to connect to all your devices, such as a cellular phone. Yet these are all are small factors compared to the following. I forced my virus to catch a microphone, a webcam, and the graphic on the display screen, you know I've created several fascinating videos. I believe some video clips will certainly be useful for you personally))

The most fascinating portion is that my application recorded is a moment you pay a visit to one of the porn web sites. I haveused two hours of my time to combine two videos, one of which is an image on the display screen and another one of the actual cam. It had been fairly amusing!

So, lets get directly to the point. I recommend you pay 300 $ to my wallet:

1N[redacted]cC

I only utilize bitcoin. If you have problems paying outjust use any search engine.

Just after getting the cash. We're going both equally just forget about this unpleasant incident and erase all the data We have collected from ur devices.

You have exactly 2 days. If I do not receive my cash, I will send out all the information to contact information I located on ur devices! Perhaps I'll do it with your social accounts . It is going to be amusing if your cherished ones receive a video footage of this type.

I offer you a small amount of time due to the fact my wallets frequently get locked and you need to send just before that. Indeed, you aren't the only individual getting an e-mail of this type, I've infected a 7664 people and a lot more than 1319 of these ended up with exciting things.

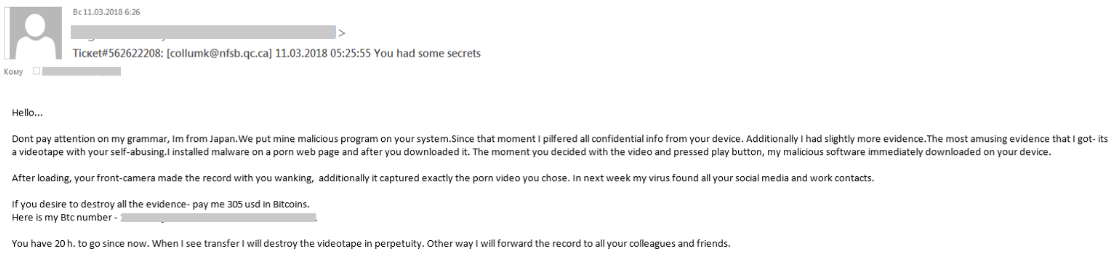
You can easily call police, believe its worthless, the worst thing they are able to perform is lock my wallet. So don't do foolish stuff.

If perhaps I will not obtain my funds for any reason, such as the failure to send them to a blocked wallet, your status will be ruined. So move!

I take care of my anonymousness and use the short-lived address to send emails, additionally I'm on the internet from my working laptop computerand i only with fake Wi-Fi from various companies apart from i use socks5. Thus, getting in touch with me and giving answers to to this notice makes no sense.

Fig.10: Screenshot of a porn-related scam e-mail (content edited for security purposes). Source: Kaspersky Security Network

The scammers claimed to have personal messages and recordings of the victim watching porn. The letters even claimed that the threat actor could combine the video that the supposed victim was watching with what was recorded through their webcam. This extortion is based purely on making threats.



Вс 11.03.2018 6:26
[redacted]>
Ticket#562622208: [collumk@nfsb.qc.ca] 11.03.2018 05:25:55 You had some secrets
Кому [redacted]

Hello...

Dont pay attention on my grammar, Im from Japan.We put mine malicious program on your system.Since that moment I pilfered all confidential info from your device. Additionally I had slightly more evidence.The most amusing evidence that I got- its a videotape with your self-abusing.I installed malware on a porn web page and after you downloaded it. The moment you decided with the video and pressed play button, my malicious software immediately downloaded on your device.

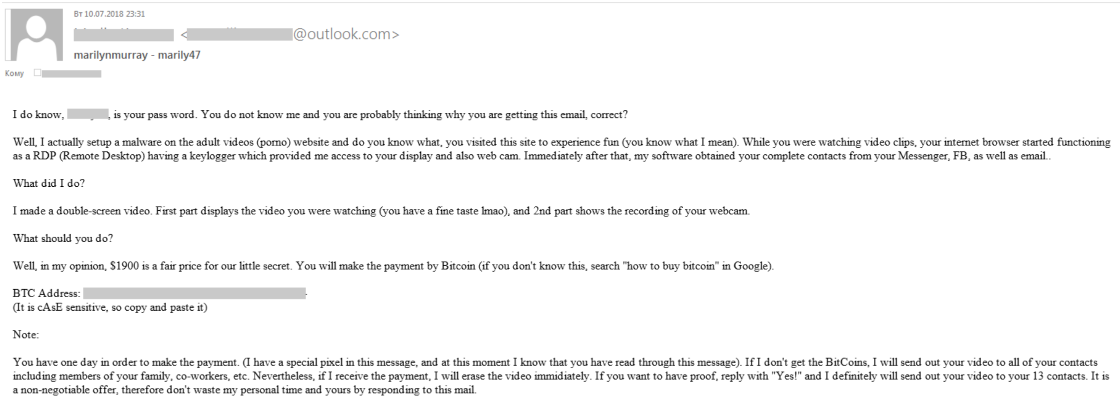
After loading, your front-camera made the record with you wanking, additionally it captured exactly the porn video you chose. In next week my virus found all your social media and work contacts.

If you desire to destroy all the evidence- pay me 305 usd in Bitcoins.
Here is my Btc number - [redacted].

You have 20 h. to go since now. When I see transfer I will destroy the videotape in perpetuity. Other way I will forward the record to all your colleagues and friends.

Fig.11: Screenshot of a porn-related scam e-mail (content edited for security purposes). Source: Kaspersky Security Network

2018, however, saw an increase in the volume of such e-mails. Moreover, they became more sophisticated and were not only threatening the user, but also 'proving' the legitimacy of the scammers claims by providing the user with actual information about them.


Вт 10.07.2018 23:31

[redacted] <[redacted]@outlook.com>

marilynmurray - marily47

Кому [redacted]

I do know, [redacted], is your pass word. You do not know me and you are probably thinking why you are getting this email, correct?

Well, I actually setup a malware on the adult videos (porno) website and do you know what, you visited this site to experience fun (you know what I mean). While you were watching video clips, your internet browser started functioning as a RDP (Remote Desktop) having a keylogger which provided me access to your display and also web cam. Immediately after that, my software obtained your complete contacts from your Messenger, FB, as well as email..

What did I do?

I made a double-screen video. First part displays the video you were watching (you have a fine taste lmao), and 2nd part shows the recording of your webcam.

What should you do?

Well, in my opinion, $1900 is a fair price for our little secret. You will make the payment by Bitcoin (if you don't know this, search "how to buy bitcoin" in Google).

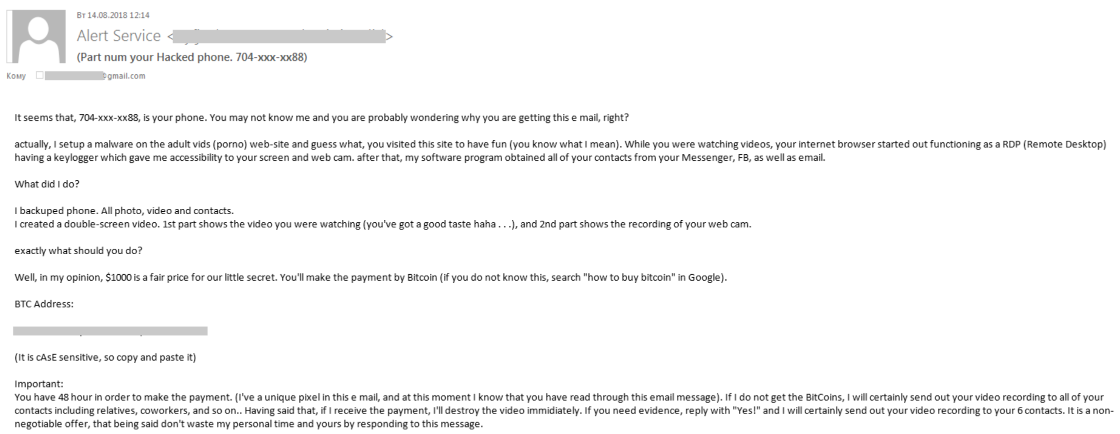
BTC Address: [redacted].
(It is cAsE sensitive, so copy and paste it)

Note:

You have one day in order to make the payment. (I have a special pixel in this message, and at this moment I know that you have read through this message). If I don't get the BitCoins, I will send out your video to all of your contacts including members of your family, co-workers, etc. Nevertheless, if I receive the payment, I will erase the video immidiately. If you want to have proof, reply with "Yes!" and I definitely will send out your video to your 13 contacts. It is a non-negotiable offer, therefore don't waste my personal time and yours by responding to this mail.

Fig.12: Screenshot of a porn-related scam e-mail (content edited for security purposes). Source: Kaspersky Security Network

In most cases, it was either a password, or a phone number, or a combination of both with an e-mail address. Since people tend to use the same passwords for different websites, the victim was often likely to believe that paired passwords and e-mail addresses found by the criminal on the dark web were authentic, even if they were not actually correct for the adult-content account in question.


Вт 14.08.2018 12:14

Alert Service <[redacted]>

(Part num your Hacked phone. 704-xxx-xx88)

Кому [redacted]@gmail.com

It seems that, 704-xxx-xx88, is your phone. You may not know me and you are probably wondering why you are getting this e mail, right?

actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I backuped phone. All photo, video and contacts.
I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, $1000 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address:

[redacted]

(It is cAsE sensitive, so copy and paste it)

Important:
You have 48 hour in order to make the payment. (I've a unique pixel in this e mail, and at this moment I know that you have read through this email message). If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on.. Having said that, if I receive the payment, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I will certainly send out your video recording to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message.

Fig.13: Screenshot of a porn-related scam e-mail (content edited for security purposes). Source: Kaspersky Security Network

Furthermore, these e-mails have been sent out in more languages than previously found.

Ср 12.09.2018 16:31

Relativamente alle questioni di sicurezza

Кому

Ciao, caro utente di .
Abbiamo installato un trojan di accesso remoto sul tuo dispositivo.
Per il momento il tuo account email è hackerato (vedi , ora ho accesso ai tuoi account).
Ho scaricato tutte le informazioni riservate dal tuo sistema e ho anche altre prove.
La cosa più interessante che ho scoperto sono i video dove tu masturbi..

Avevo incorporato un virus sul sito porno dopo di che tu l'hai installato sul tuo sistema operativo.
Quando hai cliccato su Play di un video porno, in quel momento il tuo dispositivo ha scaricato il mio trojan.
Dopo l'installazione la tua camera frontale ti filma ogni volta che tu masturbi, in più il software è sincronizzato con video che tu scegli.

Per il momento il software ha raccolto tutte le informazioni sui tuoi contatti dalle reti sociali e tutti gli indirizzi email.
Se tu vuoi che io cancelli tutti i dati raccolti, devi trasferirmi $300 in BTC (criptovaluta).
Questo è il mio portafoglio Bitcoin:
Una volta letta questa comunicazione hai 2 giorni a disposizione.

Appena hai provveduto alla transazione tutti i tuoi dati saranno cancellati..
Altrimenti manderò i video con le tue birichinate a tutti i tuoi colleghi e amici!!!

E da ora in poi stai più attento!
Per favore, visita solo siti sicuri!
Ciao!

Fig.14: Screenshot of the porn-related scam e-mail (content edited for security purposes). Source: Kaspersky Security Network

Вт 11.09.2018 19:59

Es geht um Ihre Sicherheit.

enutzer von abusix.invalid.

e RAT-Software auf Ihrem Gerät installiert.
ist Ihr E-Mail-Konto gehackt (siehe , jetzt habe ich den Zugriff auf Ihre Konten).
ertraulichen Informationen von Ihrem System heruntergeladen und ich habe weitere Beweise erhalten.
ıtesten Sachen, die ich entdeckt habe, sind Videos von Ihnen auf denen Sie masturbieren.

ien Virus auf die Pornoseite gepostet, und dann haben Sie ihn auf Ihren Betriebssystem installiert.
ı Button "Play" auf Porno-Video geklickt haben, wurde mein Trojaner in diesem Moment auf Ihr Gerät heruntergeladen.
ıllation nimmt Ihre Frontkamera jedes Mal, wenn Sie masturbieren, ein Video auf; zusätzlich wird die Software mit dem von Ihnen gewählten Video

e Software alle Ihre Kontaktinformationen aus sozialen Netzwerken und E-Mail-Adressen gesammelt.
Daten gesammelt von Ihr System löschen müssen, senden Sie mir $300 in BTC (Kryptowährung).
itcoin Wallet:
ıge nach dem Lesen dieses Briefes.

ınsaktion werde ich alle Ihre Daten löschen.
nde ich Video mit deinen Streiche an alle deine Kollegen und Freunde!!!

ın, seien Sie vorsichtiger!
n Sie nur sichere Webseiten!

Fig.15: Screenshot of a porn-related scam e-mail (content edited for security purposes). Source: Kaspersky Security Network

In reality, these mailings were based purely on the assumption that the target of such e-mails would hand over their credentials and that these would become profitable. The number of such scams grew in 2018.

PART 3 – DARKNET INSIGHTS

One of the burning topics of the adult-content industry is the controversy surrounding paid subscriptions to access websites. It is often the case that users can register for pornography accounts through a 'premium' subscription model (that includes no advertisements and unlimited access to the adult website content). Otherwise, the website they want to access does not allow them to watch any free content at all unless they pay. At most, the user may see video previews for free but still be expected to make a payment to watch the full video.

The opinions around such practice vary. Some people claim that money paid for porn "directly fuels the industry that supports the abuse, exploitation, and trafficking around the world". Others argue that pornography is like most other commodities and people are willing to exchange money for it just as they would other kinds of entertainment, such as tv-series or music. Some though prefer to highlight examples of when adult content can result in people being denied their human rights.

Whether it is worth it or not, some users agree that the price of premium accounts to popular pornography websites is rather high. For example, monthly memberships can vary from $20 to $30, and annual unlimited access costs might scale from $120 to $150. This is where cybercriminals enter the fray.

The research on porn-related cyberthreats we did previously proved that there is a very well developed supply and demand chain for stolen credentials on the dark web. We conducted research on this issue again in 2018, analyzing 20 of the top-rated Tor marketplaces listed on DeepDotWeb – an open Tor site that contains a dynamic ranking of dark markets evaluated by Tor administrators based on customers' feedback. All of them contained one to more than 3,000 offers for credentials to adult content websites. In total, 29 websites displayed more than 15,000 offers to buy one or more accounts to pornography websites (with of course, no legal guarantees of delivering on their promise).

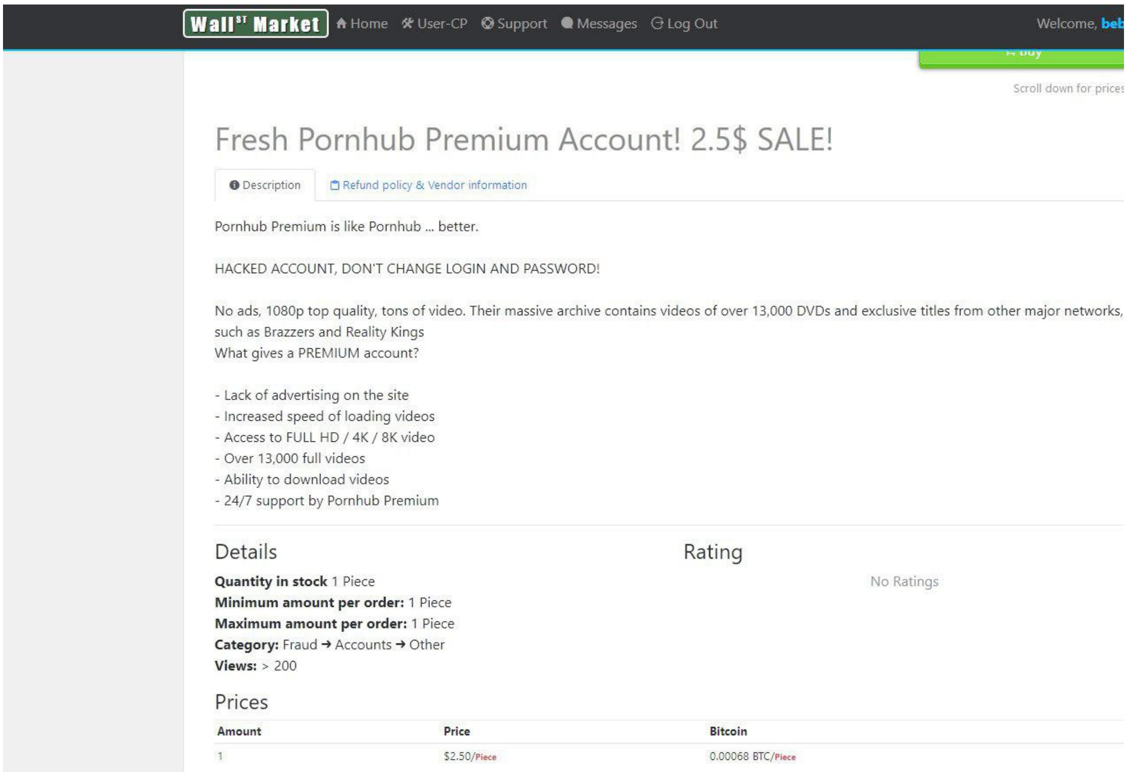


Fig.16: Example of an offer of stolen credentials on one of the Darknet's markets. Source: Kaspersky Lab

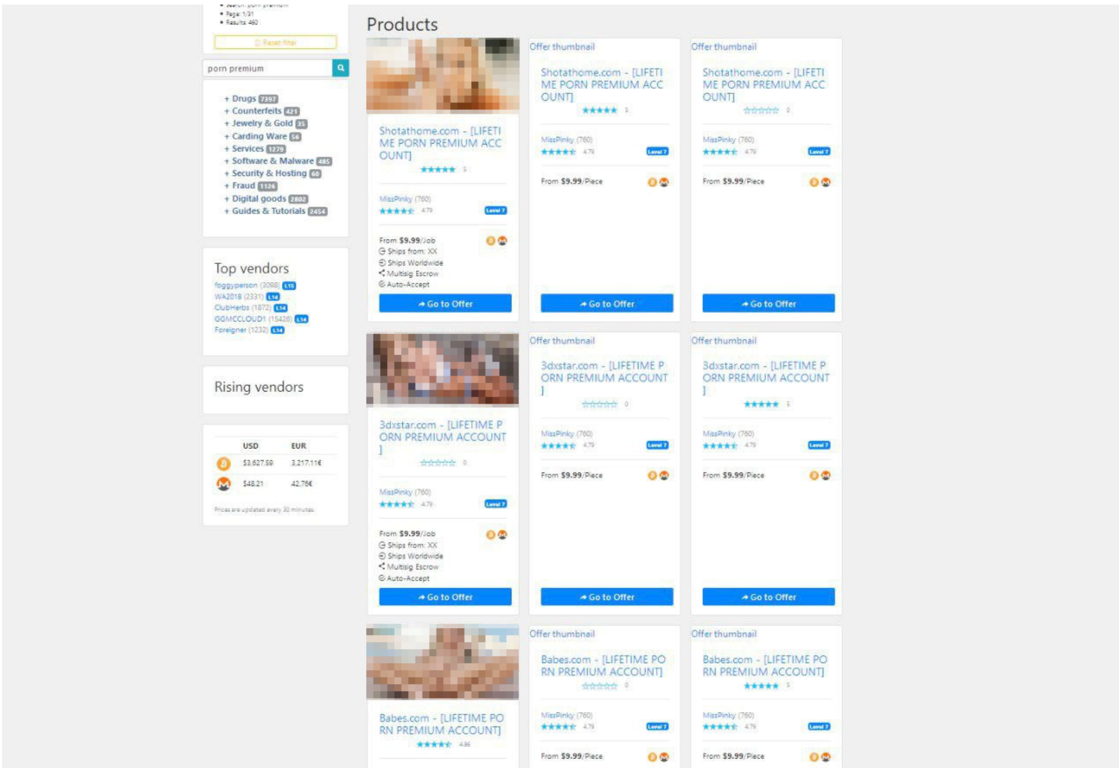


Fig.17: Examples of offers of stolen credentials on one of the Darknet's markets. Source: Kaspersky Lab

The results of the research conducted in the last year showed that four of the researched markets that offered the widest range of stolen credentials provided users with more than 5,239 unique offers. The figure for 2018 showed that their number doubled, accounting for more than 10,000 offers on sale.

The quantity of accounts available ranged from 1 to 30, with a few exceptions mostly from poorly rated sellers. However, the majority of offers promised to deliver credentials to only one account. Regardless of the type of account, the prices vary from $3 to $9 per offer, very rarely exceeding $10 – the same as back in 2017, with the vast majority of prices being limited to $6-$7 or the equal amount in bitcoins, which is 20 times cheaper than the most modest annual memberships. Getting access to an account illegally for a lower cost than a legal subscription is not the only appeal of buying such credentials on the dark web.

There is the added appeal of anonymity, hiding behind other people's credentials while watching pornography.

CONCLUSIONS AND ADVICE

Overall, the amount of downloadable malware disguised as pornography detected on users' devices significantly decreased in 2018 in comparison with record activity in 2017. While at first glance this looks like good news, a worrying trend has appeared. The number of users being attacked with malware that hunts for their pornographic content credentials is on the rise and this means premium subscriptions are now a valuable asset for cybercriminals. There is also the fact that many modern pornography websites include social functionality, allowing people to share their own private content in different ways through the website. Some people make it freely available for all, some decide to limit who can see it. There has also been a significant rise in the number of cases where people suffer from sextortion. In other words, the sphere of adult-content may contain cybersecurity challenges other than the 'classic' infected pornography websites and video files armed with malware. These challenges should be addressed properly.

Another cybersecurity risk that adult content brings, which may be less obvious, is the misuse of corporate resources. As mentioned at the beginning of this report, the unsafe consumption of pornography from the workplace may result in the corporate network being hit by a massive infection. While most malicious attacks using pornography are aimed at consumers not corporations, the fact that most consumers have job to go to every day, brings a certain risk to IT administrators responsible for securing corporate networks.

In order to consume and produce adult content safely, Kaspersky Lab advises the following:

For consumers:

- Before clicking any link, check the link address shown, even in the search results of trusted search engines. If the address was received in an e-mail, check if it is the same as the actual hyperlink.
- Do not click on questionable websites when they are offered in search results and do not install anything that comes from them.
- If you wish to buy a paid subscription to an adult content website – purchase it only on the official website. Double check the URL of the website and make sure it is authentic.
- Check any email attachments with a security solution before opening them – especially from dark web entities (even if they are expected to come from an anonymous source).
- Patch the software on your PC as soon as security updates for the latest bugs are available.

- Do not download pirated software and other illegal content. Even if you were redirected to the webpage from a legitimate website.
- Use a reliable security solution with behavior-based anti-phishing technologies – such as Kaspersky Total Security, to detect and block spam and phishing attacks.
- Use a robust security solution to protect you from malicious software and its actions – such as the Kaspersky Internet Security for Android.

For businesses:

- Educate employees in basic security hygiene, and explain the policies on accessing web sites potentially containing illegal or restricted content, as well as not opening emails or clicking on links from unknown sources.
- Businesses can also block access to web sites that contravene corporate policy, such as porn sites, by using a dedicated endpoint solution such as Kaspersky Endpoint Security for Business. In addition to anti-spam and anti-phishing, it must include application and web controls, and web threat protection that can detect and block access to malicious or phishing web addresses.